



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,608	02/11/2000	Kira Sterling Attwood	RSW00-0010	6907

36736 7590 07/18/2007
DUKE W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

07/18/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

JUL 18 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/503,608
Filing Date: February 11, 2000
Appellant(s): ATTWOOD ET AL.

Theodore D. Fay, III
Reg. No. 48,504
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 26 March 2007 appealing from the Office Action
mailed 20 October 2006.

Art Unit: 2134

(1) Real Party in Interest

A statement identifying by name the real party in interest, IBM Corporation, is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Schuba et al. U.S. Patent No. 6,725,378

Yavatkar et al. U.S. Patent No. 6,735,702

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3, 5, and 14, are rejected under 35 U.S.C. 102(e) as being anticipated by Schuba et al. U.S. Patent No. 6,725,378 (hereinafter Schuba).

Regarding claim 1, as per the first limitation, **“A method of preventing a flooding attack on a network server”** is taught in Schuba col. 1, lines 55-60 “the present invention includes a unique defense for denial of service attacks”, note denial of service is equivalent to flooding attacks;

As per the second limitation, **“in which a large number of connectionless datagrams are received for queuing to a port on the network server, comprising:”** is shown in Schuba col. 3, lines 16-33 “The Internet Protocol (IP) is the standard network layer protocol of the Internet that provides a connectionless, best effort packet delivery service. IP defines the basic unit of the data transfer used throughout an IP network, called a datagram. The deliver of datagrams is not guaranteed ... Datagrams are routed towards their destination host” {“connectionless datagrams” same as “connectionless, best effort packet delivery service” / “network server” same as “destination host”};

As per the third limitation, **“determining, in response to the arrival of a connectionless datagram from a host for a port on the network server”** is disclosed in Schuba col. 4, lines 52-54 “When a SYN packet arrives at a port on which a TCP server is listening”;

As per the fourth limitation, **“if the number of connectionless; datagrams already queued to the port from the host exceeds a prescribed threshold discarding the datagram, if the number of connectionless datagrams already queued to the port from the host**

Art Unit: 2134

exceeds the prescribed threshold” is taught in Schuba col. 4, lines 54-58 “There is a limit on the number of concurrent TCP connections that can be in a half-open connection state, called the SYN-RECVD state (i.e., SYN received). When the maximum number of half-open connections per port is reached, TCP discards all new incoming connections requests”;

As per the second limitation, **“and queuing the connectionless datagram to a queue slot of the port, if the number of connectionless. datagrams already queued to the port from the host does not exceed the prescribed threshold”** is taught in Schuba col. 4, lines 59-67 “until it has either cleared or completed some of the half-open connections”.

Regarding claim 3, this claim is directed to the apparatus of the method of claim 1 and is similarly rejected along the same rationale

Regarding claim 5, this claim is directed to a storage media containing program code of the method of claim 1 and is similarly rejected along the same rationale.

Regarding claim 14, **“wherein the computer is the network server”** is taught in Schuba col. 4, line 52 through col. 5, line 17.

Claims 2, 4, 6, and 9-13, are rejected under 35 U.S.C. 103(a) as being unpatentable over Schuba in further view of Yavatkar et al. U.S. Patent No. 6,735,702 (hereinafter Yavatkar).

Regarding claim 2, the following is not taught in Schuba: **“wherein the determining if the number of datagrams already queued to the port from the host exceeds a prescribed threshold further comprises: calculating the prescribed threshold by multiplying a percentage by the number of available queue slots for the port”** however Yavatkar teaches “A watchdog agent may assume a network attack exist if network congestion is detected ... In an

Art Unit: 2134

alternate embodiment a watchdog agent detects network congestion by monitoring interface discard counts and average queue lengths for each port on the node” in col. 15, line 63 through col. 16, line 17, note monitoring the interface for discards and average queue length is interpreted to be equivalent to calculating the prescribed threshold.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Schuba a method to protect a network from denial of service attacks to include a means to calculate the threshold limit per port. One of ordinary skill in the art would have been motivated to perform such a modification in order to gain information needed to diagnose a network attack (see Yavatkar col. 2 lines 44 et seq.) “Therefore there exists a need for a system and method allowing for the distributed state of a network such as information about attack traffic, to be quickly and accurately collected. A system and method are needed for quickly and accurately diagnosing network attacks by determining information such as the source of, or a partial path of, attack traffic”.

Regarding claim 4, this claim incorporate substantially similar subject matter as in cited in claim 2 above and is rejected along the same rationale.

Regarding claim 6, this claim incorporate substantially similar subject matter as in cited in claim 2 above and is rejected along the same rationale.

Regarding claim 9, **“further comprising: configuring a maximum number of connectionless, datagrams allowed to be queued at the port”** is taught in Yavatkar col. 12, lines 27-39 “In step 440, proactive environment 100 instantiates service object 300 based on the class of service 102. Proactive environment 100 configures service object 300 per the permissioning accessed in step 434. For example, one set of permissioning may allow agent

Art Unit: 2134

110 to use service object 300 to read the operating characteristics of port 21 and alter settings for the port”.

Regarding claim 10, **“wherein the configuring step further includes configuring a controlling percentage of available queue slots remaining for the port; and wherein the proscribed threshold is based on the controlling percentage of available queue slots remaining for the port”** is shown in Yavatkar col. 12, lines 27-39.

Regarding claim 11, **“wherein the port comprises a plurality of queue slots the method further comprising: maintaining a number of available queue slots of the plurality of queue slots for the port”** is disclosed in Yavatkar col. 12, lines 27-39.

Regarding claim 12, this claim incorporate substantially similar subject matter as in cited in claim 9 above and is rejected along the same rationale.

Regarding claim 13, this claim incorporate substantially similar subject matter as in cited in claim 10 above and is rejected along the same rationale.

(10) Response to Argument

Brief summary of prior art of records:

Schuba: discloses a method of network protection for denial of service attacks. Specifically Schuba teaches the patent in relation to the TCP/IP protocol. The Internet Protocol (IP) is the standard network layer protocol of the Internet that provides a connectionless, best effort delivery service (col. 3, lines 18-21). For any TCP connection, there are memory structures that need to allocated by both endpoints ... three memory structures need to allocated at each

Art Unit: 2134

endpoint ... There is a limit on the number of concurrent TCP connections that can be in a half-open connection state, called the SYN-RECVD state (col. 4, lines 30-65).

Yavatkar: discloses a method for diagnosing network intrusion. Specifically Yavatkar teaches a watchdog agent that determines congestion by analyzing traffic on a network.

In response to applicant's argument beginning on page 9, "*Schuba does not anticipate claim 1 because Schuba fails to disclose the feature of connectionless datagrams already queued to the port as claimed in determining, discarding, and queuing steps, ... the cited portion of Schuba teaches a method of defeating flooding attacks by limiting the number of half-open connections allowed at a given port. Schuba defines a half-open connection as a state in which the SYN datagram from a destination host has received at a source host. As shown below, a half-open connection is not the same as a queue of datagrams, contrary to any assumptions or assertion the Examiner has made. Thus, Schuba does not teach the feature of connectionless datagrams already queued to the port as claimed in determining, discarding, and queueing steps of claim 1*". The Examiner disagrees with argument and notes a connectionless datagram is explained in Schuba see col. 3, lines 16-33 "To better explain various aspects of the preferred embodiments, certain features of the Transmission Control Protocol/Internet protocol (TCP/IP) are first described. The Internet Protocol (IP) is the standard network layer protocol of the Internet that provides a connectionless, best effort packet delivery service. IP defines the basic unit of the data transfer used throughout an IP network, called a datagram. The delivery of datagrams is not guaranteed. Datagrams may be lost, duplicated, delayed, or delivered out of order. IP is connectionless, because each packet is treated independently of the others--each may

Art Unit: 2134

travel over different paths and some may be lost while others are delivered. IP provides best-effort delivery, because packets are not discarded unless resources are exhausted or underlying networks fail. Datagrams are routed towards their destination host. A set of rules characterizes how hosts and gateways should process packets, how and when error messages should be generated, and when packets should be discarded". Therefore the Examiner interprets the SYN signal or half-open connection a connectionless datagram. Half-open connections are a queue of connectionless datagrams because each SYN signal is a connectionless datagram received from the network layer (IP is a connectionless protocol). The TCP connection orientated connection is not established because the three-way handshake is not completed, a multiple of half-open connections is a queue of connectionless datagrams.

In response to applicant's argument on page 13, "In contrast, the invention of claim 1 limits the number of datagrams that are allowed to a queue at a given port. Specifically, claim 1 recites that an arriving datagram should be discarded if the number of connectionless datagram already queued to the port from the host exceeds the prescribed threshold. Schuba does not teach this claimed feature. Schuba teaches limiting the number of half-open connections by discarding new request for connections. Schuba does not teach discarding datagrams to be assigned to a queue". The Examiner disagrees with argument and notes there is no difference as explained above between "half open-connections" and the text stated in claim 1 "connectionless datagrams are received for queuing to a port". Schuba teaches all the limitations that are in claims 1, 3, 5, 7, and 14.

In response to applicant's argument beginning on page 13, "*Schuba does not teach the feature of determining, in response to the arrival of a connectionless datagram from a host for a*

port on the network server, if the number of connectionless datagrams already queued to the port from the host exceeds a prescribed threshold. Instead, Schuba counts the number of half-open connections at a port, which as described above, is entirely different than determining the number of connectionless datagrams already queued to a port". The Examiner disagrees with the argument as state above a connectionless datagram is equivalent to the half-open connection because it consists of an (IP datagram which is by definition connectionless). Counting and limiting the half-open connections is the same as determining if the connectionless datagram exceeds a prescribed threshold, the limit is the 'prescribed threshold'. The 'connectionless datagram' is the SYN request received from the network layer (i.e. an IP datagram).

In response to applicant's argument on page 14, *"Similarly, Schuba does not teach the feature of queuing the connectionless data to a queue slot of the port, if the number of connectionless datagrams already queue to the port from the host do not exceed the prescribed threshold"*. The Examiner disagrees and notes again the half-open connections are 'connectionless datagrams' as indicated by Schuba in col. 4, lines 54-67 if the maximum limit per port is reached new half-open connections are discarded, similarly if the limit is not reached the 'connectionless datagram' or 'half-open connection' would be forwarded or queued to the port.

In response to applicant's argument beginning on page 14, *"A.2. Rebuttal to Examiner's Responses In response to the facts established above regarding the feature of connectionless datagrams already queued to the port as claimed in the determining, discarding, and queueing steps, ... Schuba does not teach the feature of connectionless datagrams already queued to the port as claimed in determining, discarding, and queueing steps because a half-open connection*

Art Unit: 2134

request is not the same as a queue of datagrams. Schuba instead teaches discarding incoming connection request until the maximum number of half-open connection is reduced". The Examiner disagrees with argument incoming connection request would be an IP datagram or datagrams (assuming multiple requests as described in Schuba). These incoming request in Schuba are equivalent to a 'queue of connectionless datagrams', which are discarded until the number of allowed request or 'connectionless datagrams' is below the prescribed limit see Schuba col. 4, lines 52-67.

In response to applicant's arguments beginning on page 15, *"Several important differences exist between discarding additional connection requests, as in Schuba, no queue for the datagrams themselves has been described. Instead, Schuba refers to a half-open backlog queue ... One of ordinary skill would instantly recognize the difference between discarding a datagram queued at a port and removing connection from a half-open backlog queue ... A half-open connection is not a datagram, even if a half-open connection is created using datagrams. Schuba only teaches methods for dealing with too many half-open connections, which is entirely distinct from discarding datagrams queued at a port. The fact that the half-open connection are created with connectionless datagrams is wholly irrelevant to this distinction"*. The Examiner disagrees with applicants logic and reiterates the following a half-open connection is a connectionless datagram received from the IP layer. Schuba teaches discarding these 'half open connections' or 'connectionless datagrams' when a limit is reached at a port.

In response to applicant's argument beginning on page 16, *"However, the Examiner misconstrues Applicant's arguments ... The thrust of Applicant's argument is that a fundamental and marked difference exist between a queue of connectionless datagrams at a port, as claimed*

Art Unit: 2134

and a queue of half-open connections, as described in Schuba ... Additionally, the Examiner does not offer any support for the Examiner's assertions". The Examiner disagrees with applicant's interpretation of responses and states: First, "Anyone of ordinary skill in the art" understands that the half-open connection is a received, SYN connection request which is a connectionless datagram received from the network layer. Second, Schuba teaches the connectionless datagram col. 3, lines 16-33 "To better explain various aspects of the preferred embodiments, certain features of the Transmission Control Protocol/Internet protocol (TCP/IP) are first described. The Internet Protocol (IP) is the standard network layer protocol of the Internet that provides a connectionless, best effort packet delivery service. IP defines the basic unit of the data transfer used throughout an IP network, called a datagram. The delivery of datagrams is not guaranteed. Datagrams may be lost, duplicated, delayed, or delivered out of order. IP is connectionless, because each packet is treated independently of the others--each may travel over different paths and some may be lost while others are delivered. IP provides best-effort delivery, because packets are not discarded unless resources are exhausted or underlying networks fail. Datagrams are routed towards their destination host. A set of rules characterizes how hosts and gateways should process packets, how and when error messages should be generated, and when packets should be discarded". This was cited in the previous Office Action, see page 5.

In response to applicant's arguments beginning on page 17, *"The Examiner asserts that discarding datagrams queued at a port is the same as discarding too many half open connection because a TCP/IP connection requires a three-way handshake and because TCP/IP transfer connectionless datagrams. However, the Examiner's responses ignores the fact that a queue of*

Art Unit: 2134

half-open connections, as in Schuba, is still fundamentally different than a queue of connectionless datagrams, as in claim 1. The Examiner's assertion to the contrary is plainly wrong". The Examiner disagrees with applicant's interpretation, the Examiner reiterates the following points:

- a half-open connection is a 'connectionless datagram'
- multiple half-open connections is a 'queue of connectionless datagrams'
- Listening for incoming SYN packets and determining if a limit is reached is 'determining the number of connectionless datagrams', because a SYN packet is a connectionless datagram.

In response to applicant's arguments beginning on page 18, *"The second ground of rejection is whether the Examiner failed to state a prima facie obviousness rejection against claims 2, 4, 6, and 9-13 under 35 U.S.C. § 103(a) over Schuba in view of Yavatkar et al., Method and System for Diagnosing Network Instructions, U.S. Patent 6,735,701, August 31, 1999 (hereinafter "Yavatkar") ... Applicants first respond to the rejection by showing that the proposed combination, when considered as a whole, does not teach or suggest all of the features of claim 2 ... The Examiner failed to state a prima facie obviousness rejection against claim 2 because the proposed combination when considered as whole, does not teach or suggest all the feature of claim 2. As shown in Section A, Schuba does not teach all of the claimed features of claim 1 ... Yavatkar fail to teach or suggest any features of claim 1".* The Examiner disagrees as stated above Schuba teaches claim 1.

Art Unit: 2134

In response to applicant's argument beginning on page 20, *"Additional, neither Schuba nor Yavatkar teach or suggest the features of calculating the prescribed threshold by multiplying a percentage by the number of available queue slots for the port ... Neither the cited portion nor any other portion teaches or suggest the feature of calculating the prescribed threshold by multiplying a percentage by the number of available queue slots for the port ... Scuba fails to cure the deficiencies of Yavatkar"*. The Examiner does not agree with applicant's argument. The Examiner interprets percentage to be as defined by applicant's specification on page 4, lines 7-13 *"The maximum number of datagrams and the threshold percentage P will be difficult for most owners to configure. Therefore, a "statistics" mode is provided that measures normal traffic loads of different servers and suggests an appropriate maximum and threshold that will not hamper similar legitimate traffic loads. This statistics mode is not part of the claimed invention and is not described further herein"*. Therefore using an average which is a statistical mode is equivalent to the meaning of the claimed percentage. See Yavatkar col. 15, line 63 through col. 16, line 17, *"In an alternate embodiment a watchdog agent detects network congestion by monitoring interface discard counts and average queue lengths for each port on the node"*. An average as well as the level are both calculations of the amount of datagrams received or dropped by a port.

In response to applicant's argument beginning on page 22, *"The Examiner Failed to State a Proper Motivation, Teaching, or Suggest to Combine the References ... However, the hypothetical advantage proposed by the Examiner, namely, "to gain information needed to diagnose a network attack," does not actually exist because Schuba already teaches a way to gain information to diagnose a network attack"*. The Examiner disagree with applicant and

Art Unit: 2134

notes the motivation as stated above and in the Office Action is appropriate, in addition the invention of Yavatkar and Schuba are both directed to the same field of endeavor detecting attacks network attacks such as SYN flooding.

In response to applicant's argument beginning on Page 24, *"The Proposed Combination Changes the Principle of Operation of Schuba ... The cited portion discloses that the monitoring resource 51 executes a monitor program 52 which performs various network monitoring functions, including examining packets. Schuba nowhere discloses that the monitoring program 52 may move from monitoring resource to monitoring resource ... Monitoring the network by any principle other than that described in Schuba, such as by deploying mobile software modules, would modifying, altering, or replacing the principle of operation of Schuba's invention"*. The Examiner disagrees and notes that the both Schuba and Yavatkar are directed to monitoring the network in order to detect network attacks, in addition Schuba teaches in col. 7, lines 10-16 "It is preferred that monitoring resource 51 be in the form of a programmable digital computer that is operable to execute monitor 52. Monitoring resource 51 may be in the form of a single processing unit operatively coupled to network 22 or a distributed system of different units operatively coupled to network 22, as would occur to those skilled in the art" that the monitoring may be distributed.

In response to applicant's arguments beginning on page 26, *"Claims 9 and 12 ... Because neither Schuba nor Yavatkar teach or suggest all of the features or claim 1 ... In addition, claim 9, claims other additional combination of features not disclosed by either Schuba or Yavatkar"*. The Examiner disagrees, Schuba teaches claim 1 as noted above. Furthermore

Art Unit: 2134

claim 9, "configuring the maximum number of connectionless, datagrams allowed to be queued at the port" is taught in Yavatkar col. 12, lines 27-39 the agent may alter the setting on a port, these settings are obviously deal with methods to prevent attacks, such as altering the maximum number of connections allowed to a port.

In response to applicant's argument beginning on page 29, *"No Proper Teaching, Motivation, or Suggestion Exists to Combine the References as Proposed by the Examiner"*. The Examiner disagrees as stated above the motivation as stated above and in the Office Action is appropriate, in addition the invention of Yavatkar and Schuba are both directed to the same field of endeavor detecting attacks network attacks such as SYN flooding.

In response to applicant's argument beginning on page 31, *"Claims 10 and 13 ... Because neither Schuba nor Yavatkar teach or suggest all of the features of claim 9 ... In addition, claim 10 claims other additional combinations of features not disclosed by either Schuba or Yavatkar"*. The Examiner disagrees and notes that claim 10 is taught in Yavatkar col. 12, lines 27-39 the agent may alter the setting on a port, these settings are obviously deal with methods to prevent attacks, such as altering the maximum number of connections allowed to a port.

In response to applicant's argument beginning on page 33, *"No Proper Teaching, Motivation, or Suggestion Exists to Combine the References as Proposed by the Examiner"*. The Examiner disagrees as stated above the motivation as stated above and in the Office Action is appropriate, in addition the invention of Yavatkar and Schuba are both directed to the same field of endeavor detecting attacks network attacks such as SYN flooding.

Art Unit: 2134

In response to applicant's arguments beginning on page 34, "*Claim 11 ... because neither Schuba nor Yavatkar teach or suggest all of the features of claim 1*". The Examiner disagrees, Schuba teaches claim 1 as noted above.

In response to applicant's argument beginning on page 35, "*No Proper Teaching, Motivation, or Suggestion Exists to Combine the References as Proposed by the Examiner*". The Examiner disagrees as stated above the motivation as stated above and in the Office Action is appropriate, in addition the invention of Yavatkar and Schuba are both directed to the same field of endeavor detecting attacks network attacks such as SYN flooding.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,



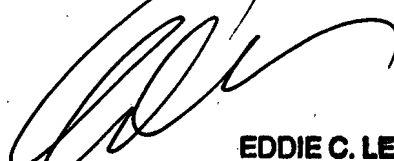
ET
Ellen Tran

Conferees:

Kambiz Zand


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Eddie Lee


EDDIE C. LEE
SUPERVISORY PATENT EXAMINER